

What must be documented	ISO 27001 reference	Usually documented through
Scope of the ISMS	Clause 4.3	ISMS Scope document
Information security policy	Clause 5.2	Information Security Policy
Risk assessment and risk treatment process	Clause 6.1.2	Risk Assessment and Treatment Methodology
Statement of Applicability	Clause 6.1.3 d)	Statement of Applicability
Risk treatment plan	Clauses 6.1.3 e, 6.2, and 8.3	Risk Treatment Plan
Information security objectives	Clause 6.2	List of Security Objectives
Risk assessment and treatment report	Clauses 8.2 and 8.3	Risk Assessment & Treatment Report
Inventory of assets	Control A.5.9*	Inventory of Assets, or List of Assets in the Risk Register
Acceptable use of assets	Control A.5.10*	IT Security Policy
Incident response procedure	Control A.5.26*	Incident Management Procedure
Statutory, regulatory, and contractual requirements	Control A.5.31*	List of Legal, Regulatory, and Contractual Requirements
Security operating procedures for IT management	Control A.5.37*	Security Procedures for IT Department
Definition of security roles and responsibilities	Controls A.6.2 and A.6.6*	Agreements, NDAs, and specifying responsibilities in each security policy and procedure
Definition of security configurations	Control A.8.9*	Security Procedures for IT Department
Secure system engineering principles	Control A.8.27*	Secure Development Policy
Trainings, skills, experience, and qualifications	Clause 7.2	Training Certificates, Training Manuals, Training Plan and Attendance List
Monitoring and	Clause 9.1	Measurement Report/Reporting

What must be documented	ISO 27001 reference	Usually documented through
measurement results		Dashboards
Internal audit program	Clause 9.2	Internal Audit Program
Results of internal audits	Clause 9.2	Internal Audit Report
Results of the management review	Clause 9.3	Management Review Minutes and Action Tracker with the agreed actions, responsibility and timelines.
Results of corrective actions	Clause 10.2	Corrective Action Report/Tracker
Logs of user activities, exceptions, and security events	Control A.8.15*	Automatic logs in information systems

Statement of Applicability

Provides a description of selected and implemented controls along with the justifications for any exclusions.



Other Documents include: -

- Procedure for Document and Record Control (clause 7.5, control A.5.33)-Control of Documented Information Procedure
- Procedure for Internal Audit (clause 9.2)-This may include the Internal Audit Charter
- Procedure for Corrective Action (clause 10.2)
- Information Classification Policy/Procedure (controls A.5.10, A.5.12, and A.5.13)
- Information Transfer Policy (control A.5.14)
- Access Control Policy (control A.5.15)
- Password Policy (controls A.5.16, A.5.17, and A.8.5)

- Supplier Security Policy (controls A.5.19, A.5.21, A.5.22, and A.5.23)
- Disaster Recovery Plan (controls A.5.29, A.5.30, and A.8.14)
- Mobile Device, Teleworking, and Work from Home Policy (controls A.6.7, A.7.8, A.7.9, and A.8.1)
- Procedures for Working in Secure Areas (controls A.7.4 and A.7.6)
- Clear Desk and Clear Screen Policy (control A.7.7)
- Bring Your Own Device (BYOD) Policy (controls A.7.8 and A.8.1)
- Material Disposal and Destruction Policy (controls A.7.10, A.7.14, and A.8.10)
- Backup and Restoration Policy (control A.8.13)
- Encryption Policy (control A.8.24)
- Change Management Policy/Procedure (control A.8.32)